#4228

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita
Art. 25 GDPR

Avv. Nicola Fabiano
Commissione Privacy CNF
GdL FIIF-CNF

SL FABIANO

Outline

1. **Introduzione storica**
   - ☑ Disciplina della Direttiva 95/46/CE
   - ☑ Dalle PETs alla Privacy by Design
   - ☑ La 32ma conf. int.le Garanti e la risoluzione su Privacy by Design
2. **Dati personali a rischio ? Big Data**
   - ☑ Il fenomeno Big Data
3. **GDPR e Data Protection by Design and by Default**
   - ☑ Analisi dell'art. 25
   - ☑ Qualificazione dei principi
   - ☑ Obbligo di protezione dei dati
   - ☑ Pseudonimizzazione e minimizzazione
   - ☑ Tecniche di anonimizzazione e pseudonimizzazione
   - ☑ Rischi per l'anonimizzazione ? Attacchi ed effetti
   - ☑ Differential privacy
4. **Internet of Things e Blockchain**
   - ☑ IoT e i fenomeni "smart"
   - ☑ IoT ecosystem: blockchain as a service
   - ☑ Profili connessi alla data protection

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

(C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

DIRETTIVA 95/46/CE

(26) considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile;
che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona;
che **i principi della tutela non si applicano a dati resi anonimi** in modo tale che la persona interessata non è più identificabile;
che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata;

DIRETTIVA 95/46/CE

Art. 6

Gli Stati membri dispongono che i dati personali devono essere:

…

e) conservati in modo da consentire l' identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successiva mente trattati. Gli Stati membri prevedono garanzie adeguate per i **dati personali conservati oltre il sud detto arco di tempo per motivi storici, statistici o scientifici**.

CONVENZIONE 108

Articolo 5 – Qualità dei dati

I dati a carattere personale oggetto di elaborazione automatica devono essere:

…

e) conservati sotto una forma che permetta l'identificazione delle persone interessate **per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati**.

PROTOCOLLO ESPLICATIVO CONV. 108

Article 5 – Quality of data

42. The requirement appearing under littera e concerning the time-limits for the storage of data in their name-linked form does not mean that **data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers**.

42. Il requisito che appare sotto la lettera e riguardante i termini per la memorizzazione dei dati nella loro forma concatenata non significa che dopo qualche tempo i dati dovrebbero essere irrevocabilmente separati dal nome della persona a cui si riferiscono, **ma solo che non dovrebbe essere possibile collegare prontamente i dati e gli identificatori**.

Inquadramento storico

Nel 1995 con un documento congiunto dal titolo "***Privacy-enhancing technologies: the path to anonymity***" la Commissioner dell'Ontario (Canada) e la Dutch DPA (Autorità Olandese) iniziano a parlare di

Privacy Enhancing Technologies - PET(s)

Definizione di PET

Privacy-Enhancing Technologies (PETs) can be defined as **technologies that are enforcing privacy principles in order to protect and enhance the privacy** of users of information technology (IT) and/or of individuals about whom personal data are processed (the so-called data subjects).

IL CODICE PRIVACY (D.LGS. 196/2003)

Art. 3 - Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici **sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi**, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od **opportune modalità che permettano di identificare l'interessato solo in caso di necessità**.

LA POSIZIONE DELLA COMMISSIONE UE

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET) del 2.5.2007

COM. COMMISSIONE UE

2. CHE COSA SONO LE TECNOLOGIE PET ?

Esistono diverse definizioni delle PET nell'ambito della comunità accademica e dei progetti pilota in questo settore. Secondo il progetto PISA finanziato dalla CE, ad esempio, **con PET si intende un sistema coerente di misure nel settore delle TCI che tutela la privacy sopprimendo o riducendo i dati personali ovvero evitando un qualunque trattamento innecessario e/o indesiderato dei dati personali, preservando al contempo la funzionalità del sistema di informazione.**

L'uso delle PET può contribuire all'ideazione di sistemi e servizi di informazione e comunicazione che permettono di ridurre al minimo la raccolta e l'uso di dati personali e di favorire il rispetto delle norme sulla protezione dei dati.

La Commissione, nella sua prima relazione sull'attuazione della direttiva relativa alla protezione dei dati, ha affermato che "*l'utilizzo di misure tecnologiche appropriate costituisce un compromesso essenziale agli strumenti giuridici e dovrebbe costituire parte integrante di qualunque sforzo volto a conseguire un livello sufficiente di tutela della privacy* ...".

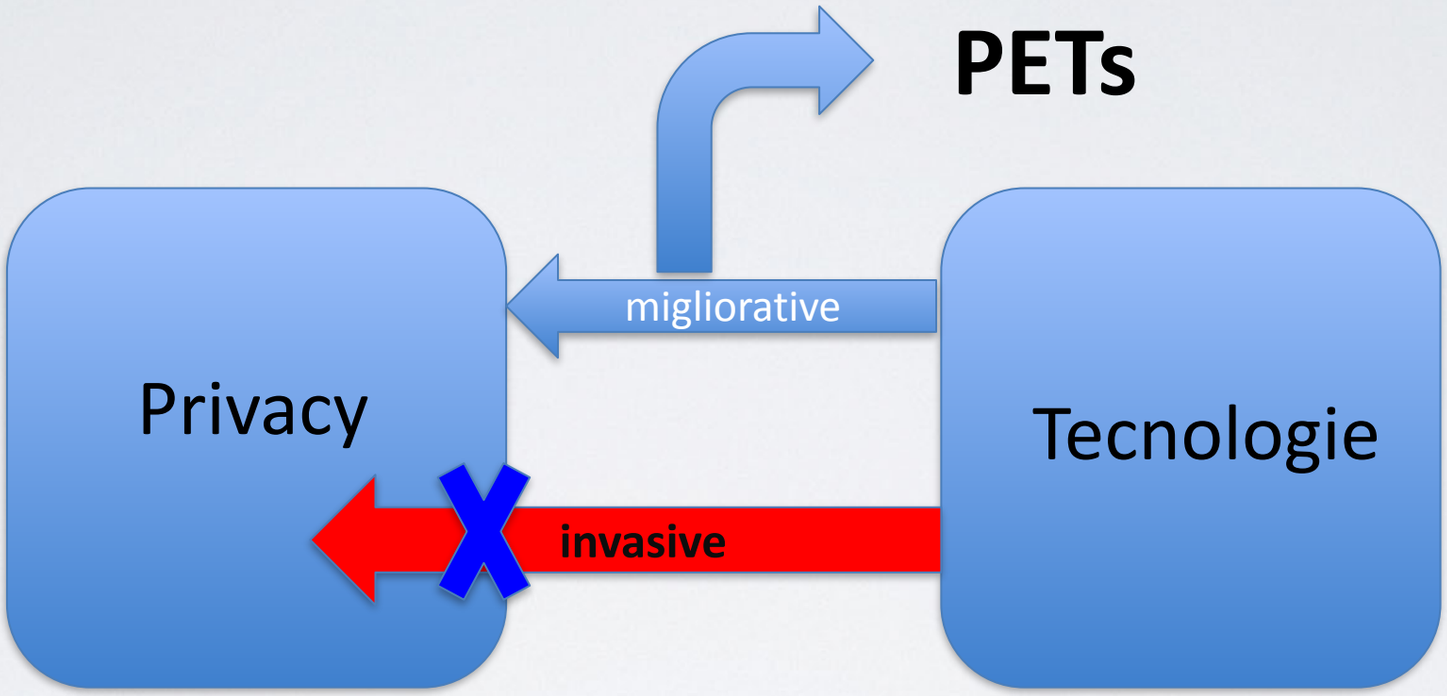
L'uso delle tecnologie PET dovrebbe consentire di contrastare le violazioni di talune norme sulla protezione dei dati o di contribuire al loro rilevamento.

COMMISSIONE UE

Si possono citare svariati esempi di tecnologie PET:

- *Ripristino automatico dell'anonimato dopo un determinato periodo di tempo, a suffragio del principio in base al quale i dati trattati dovrebbero essere archiviati in modo tale da permettere l'identificazione delle persone interessate solo per il tempo strettamente necessario a conseguire gli scopi per i quali erano stati raccolti.*
- *Strumenti di crittaggio volti a prevenire la pirateria informatica quando l'informazione è trasmessa via Internet, i quali rafforzano l'obbligo che incombe ai responsabili del trattamento di adottare misure adeguate per proteggere i dati personali dal trattamento illecito.*
- *Dispositivi per bloccare i marcatori (cookie), installati nel computer dell'utente per l'esecuzione di talune istruzioni senza che l'interessato ne sia consapevole, i quali rafforzano il rispetto del principio che i dati devono essere trattati secondo modalità eque e legittime, e che le persone interessate devono essere informate del trattamento in corso.*
- *Lo standard P3P (Platform for Privacy Preferences), che consente agli utenti Internet di analizzare l'informativa sulla privacy dei siti web e di compararla alle proprie preferenze circa le informazioni che desiderano diffondere, contribuisce a garantire che gli interessati autorizzino il trattamento dei loro dati con cognizione di causa.*

PETs



L’interessato deve essere sempre in grado di poter controllare l’utilizzo delle informazioni personali

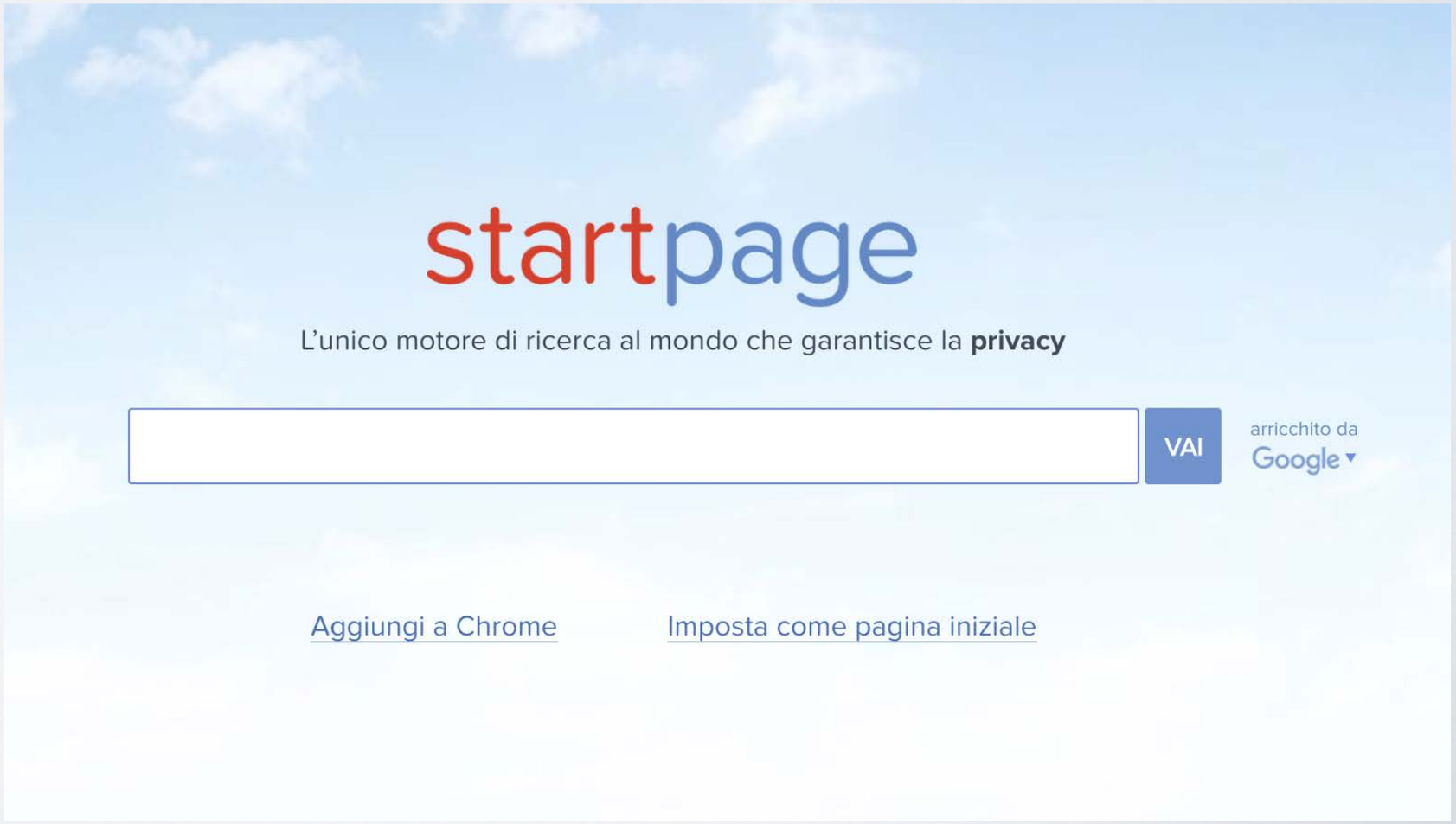
Alcuni esempi di PETs

- PGP o S/MIME per criptare messaggi email
- Truecrypt - http://www.truecrypt.org per criptare dati
- TOR - http://www.torproject.org per l'anonimato nella navigazione in rete
- Sistemi per criptare dati biometrici
- Tecnologia RFID
- Sistemi per criptare le immagini (es. videosorveglianza)
- Sistemi per il controllo delle reti e degli accessi (ISPs – AdS) – dati criptati
- Sistemi che assicurino l'effettiva cancellazione dei dati dei body-scanner
- Sistemi per il corretto uso delle identità digitali (autenticazione)
- Sistemi e procedure idonee a consentire il controllo dei propri dati e a migliorare i livelli di sicurezza nel trattamento dei dati personali (es. DuckDuckGo)
- Gestione della identità (IDM – Identity Managment)

…

In generale qualsiasi soluzione tecnologica che provveda ad aumentare il controllo ed i livelli di sicurezza dei dati personali.

Alcuni esempi di PETs



DuckDuckGo Search Engine

Guest

Duck Duck Go, Inc. [US] | https://duckduckgo.com

Privacy, simplified.

DuckDuckGo

The search engine that doesn't track you. Learn More.

About Tor

Tor Browser | Search or enter address

Search

Most Visited | Learn more about ... | The Tor Blog

Search | Web Search | Highlight

Tor Browser
7.5

Welcome to Tor Browser

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with DuckDuckGo.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

- Tips On Staying Anonymous »
- Tor Browser User Manual »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

Lo scenario internazionale

- La 32^ Conferenza mondiale dei Garanti ha adottato la risoluzione – proposta dalla Commissioner dell'Ontario Ann Cavoukian – sulla **Privacy by Design** (32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel 27-29 October, 2010 - **Resolution on Privacy by Design**).

- La Commissione Europea con la COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI - Un approccio globale alla protezione dei dati personali nell'Unione europea del 4.11.2010 COM(2010) 609 definitivo propone una strategia per rafforzare le norme sulla protezione dei dati dell'UE.

*La raccolta e l'utilizzo dei dati personali **siano limitati allo stretto necessario**.*
*Gli interessati devono essere informati in modo chiaro e trasparente **su come, perché e da chi i loro dati sono raccolti e utilizzati**. Essi dovrebbero essere in grado di esprimere un consenso informato al trattamento, ad esempio quando surfano in internet, e avere il "diritto all'oblio" quando i propri dati non sono più necessari o se vogliono farli cancellare.*

Privacy by Design

COMPONENTI DELLA PbD

1) Information Technologies

2) Pratiche commerciali responsabili

3) Progettazione di strutture ed ambienti

7 Principi della PbD

1) **Proactive:** approccio proattivo piuttosto che reattivo; l'obiettivo è quello di anticipare gli eventi e non attendere che essi si verifichino per proporre rimedi alle soluzioni.
2) **By Default**: salvaguardia del soggetto poiché il bene "privacy" va considerato a priori; nessuna azione è richiesta all'interessato per proteggere la propria privacy.
3) **Embedded**: è incorporata nell'architettura dei sistema e delle pratiche commerciali e non costituisce un *quid pluris*.
4) **Positive – Sum**: mira a conciliare tutti gli interessi legittimi e gli obiettivi in una somma positiva del tipo "win-win" dove sono inutili i compromessi e non attraverso un approccio datato del tipo "zero-sum".
5) **Lifecycle Protection**: incorporati i dati all'inizio non c'è rischio sino alla fine del processo di trattamento dei dati (distruzione in modo sicuro).
6) **Visibility and Transparency**: garantisce che tutti i soggetti interessati in qualsiasi momento effettuare potranno effettuare le verifiche più opportune in assoluta trasparenza.
7) **Respect of user privacy**: richiede agli operatori che gli interessi dei soggetti siano preminenti; approccio *user-centric*.

In Europa

La Commissione Europea con la COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI - Un approccio globale alla protezione dei dati personali nell'Unione europea del 4.11.2010 COM(2010) 609 definitivo **propone una strategia** per rafforzare le norme sulla protezione dei dati dell'UE.

La raccolta e l'utilizzo dei dati personali ***siano limitati allo stretto necessario****.*
Gli interessati devono essere informati in modo chiaro e trasparente ***su come, perché e da chi i loro dati sono raccolti e utilizzati****. Essi dovrebbero essere in grado di esprimere un consenso informato al trattamento, ad esempio quando surfano in internet, e avere il "diritto all'oblio" quando i propri dati non sono più necessari o se vogliono farli cancellare.*

Big Data

Internet e Big Data:

uso consapevole delle risorse digitali nel rispetto dei diritti alla riservatezza e alla protezione dei dati personali

SL FABIANO

Il dato è un diritto fondamentale in EU

Il dato non può costituire controprestazione (v. art. 3, comma 1, della **proposta di** DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativa a determinati aspetti dei contratti di fornitura di contenuto digitale del 9/12/2015 **-** Opinion EDPS n. 4/2017).

data does good How It Works Security About Us FAQ Causes Blog Join Now

How it works:

We help you take control of your data and raise money for charity - without costing you a penny.

Order Date	Title	Category	Price
10/15/14	Twin Peaks: Season 2	DVD	$11.22
11/30/14	Charmin Ultra Soft Bathroom Tissue 9 Family Rolls	Health and Beauty	$10.99
2/27/15	Look And Feel Canadian Breath Spray	Health and Beauty	$7.53
9/6/15	Complete Business Statistics	Hardcover	$10.24
9/7/15	American Crew: Classic Fiber, 3 oz (2 pack)	Apparel	$15.49
9/20/15	Tweezerman G.E.A.R. Moustache Scissors with Comb	Health and Beauty	$14.63
9/20/15	Proctor Silex 22611 2-Slice Toaster	Kitchen	$12.99
9/20/15	Wahl 9854-600 Lithium Ion All In One Trimmer	Health and Beauty	$38.94
9/20/15	Brush Strokes Two-sided Boar Bristle Brush	Misc.	$3.94

Fig. 1: The REAL shopping history of one of our founders. (Hint: you can tell he likes grooming...)

When you shop online, you generate data about your online shopping history. This data is a valuable resource you own!

Just how valuable is your data? Well, big tech companies are getting rich on it. But it's your data, and you have a right to do what you want with it!

We make it possible for you to turn your **anonymous** online shopping history into a cash donation to any nonprofit. Simply add our secure browser extension, and everytime you shop, anonymous data will be shared with us.

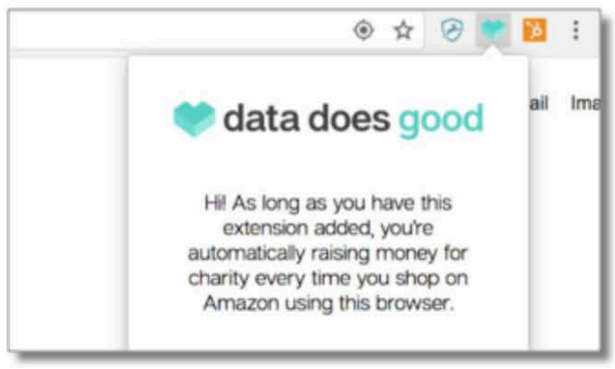


Fig. 2: Our lightweight and secure extension.

Il dato è un diritto fondamentale in EU

data does good How It Works Security About Us FAQ Causes Blog Join Now

Our promise:

Your shopping information is only used to reveal general online shopping trends for brands.

That means your data is kept 100% anonymous, private, and secure.

All shopping history we receive is totally anonymous. We do not collect or store any personal information, like name or address, in connection with your shopping history.

You will never receive any targeted advertisements or spam as a result of joining. The only information we share is to help brands better understand shopping trends.

All potentially sensitive information is protected using three layers of security. We stay ahead of best practices in the industry.

Il dato è un diritto fondamentale in EU

Personal information. You can visit our Site without submitting any information such as a name or email address that we can directly associate with a specific person. However, if you use certain features on the Site, such as to register to use our Services, you will be required to provide personal information. This information may include details such as your:

- Name;
- Email address;
- Home address;
- Shipping address;
- Referral information; and
- Login credentials for any online shopping accounts with third parties that you choose to associate with our Services.

We may also ask for additional information about you, including your occupation, your month and year of birth, and demographic information. This may include information about your gender, household income, and race. We may ask for additional demographic information after you have registered as a user, and you may have the opportunity to provide us with additional information in connection with your account.

In order to provide our Services, we may, at your direction, collect personal information about you from third-party sources. For example, if you provide us with certain login credentials, we may retrieve information about your online shopping and browsing history at retailers from third-party brands and online retailers. You may also submit your online shopping and browsing history to us manually.

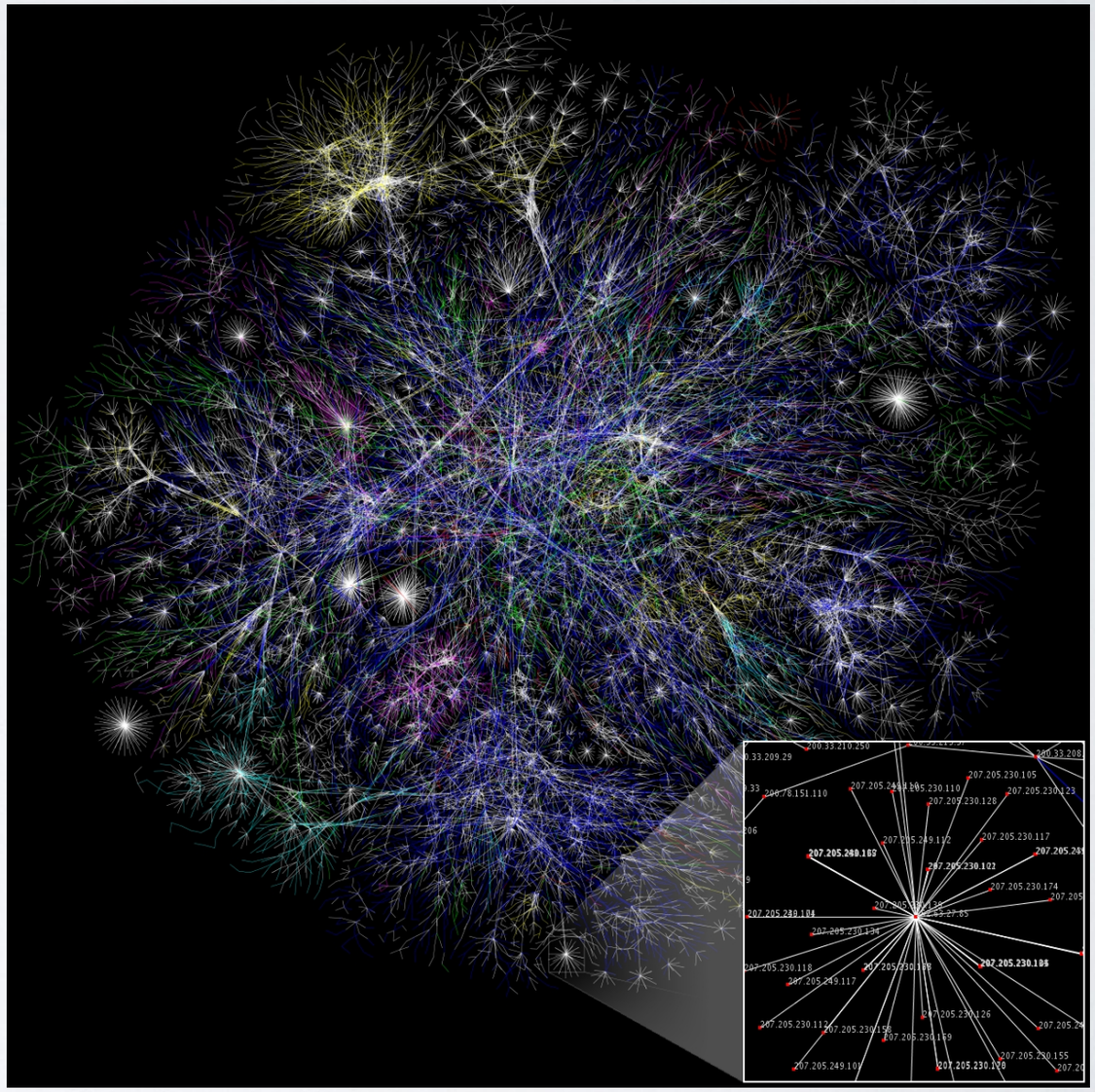
You may also download a browser extension from our website that will automatically collect and provide us with information about your online shopping and browsing history at retailers' websites. The browser extension collects and relays to us information on an ongoing basis. Once installed, the browser extension will automatically collect this information; you do not need to enable or configure it. The browser extension Does Not Send Us Information About *All* Of Your Online Browsing Activity, just your activity at certain specified retailers' sites, which the browser extension detects by reading the URL for the websites you visit.

Your online shopping and browsing history may include a wide range of data, including the following:

- Customer name;
- Customer email address;
- Shipping name and address;
- Payment data, including partial payment card numbers;
- Order information, including the title, category, and price of the product;
- Web browsing behavior on retailers' websites, including searches conducted, pages viewed (including the pages' URLs), items viewed, orders placed, order status, package feedback, product reviews, and recommendations from the retailers; and
- Metadata associated with your online shopping and web browsing behavior on retailer's websites, including the date and time of your browsing activity, the type of browser you use, and the other data elements listed under the "onCompleted" heading here: https://developer.chrome.com/extensions/webRequest#event-onCompleted.

At our discretion, we also may obtain information about you from other sources. This could include information that is publicly available or that is available from data providers or retailers you have visited, and we may combine such information with personal information we collect from you. We may analyze this personal information and any non-personal information we have collected to draw other demographic conclusions about or infer the commercial interests of our users.

Siamo capaci di guardare ciò che accade fuori ?



3,719,963,242

Internet Users in the world

1,248,651,406

Total number of Websites

173,991,110,301

Emails sent today

3,978,602,736

Google searches today

3,729,683

Blog posts written today

494,419,101

Tweets sent today

4,510,653,568

Videos viewed today
on YouTube

51,119,192

Photos uploaded today
on Instagram

81,840,407

Tumblr posts today

The Internet in Real Time

By the time you finish reading this sentence, there will have been 219,000 new Facebook posts, 22,800 new tweets, 7,000 apps downloaded, and about $9,000 worth of items sold on Amazon… depending on your reading speed, of course. Now that the Internet is widely available, just one second of global online activity is jam-packed full of events, from communication with others to data storage to entertainment options galore.

For example, in the amount of time you've been on this page, this is how much data has already passed through the Internet.

321,600

GIGABYTES OF DATA

The amount of data uploaded to the Internet in a single second is a staggering 24,000 gigabytes. Cisco forecasts that monthly Internet data will reach 91.3 exabytes – or 1 billion gigabytes – by the year 2016, pushing the amount of online activity even higher.

I multipli del byte secondo le unità del Sistema Internazionale (SI) delle unità di misura

Nome	Simbolo	Multiplo
Kilobyte	KB	10^3
Megabyte	MB	10^6
Gigabyte	GB	10^9
Terabyte	TB	10^{12}
Petabyte	PB	10^{15}
Exabyte	EB	10^{18}
Zettabyte	ZB	10^{21}
Yottabyte	YB	10^{24}

Big Data

Big data *è il termine usato per descrivere una raccolta di dati così estesa in termini di* ***volume****,* ***velocità*** *e* ***varietà*** *da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore.*

Big data rappresenta anche l'interrelazione di dati provenienti potenzialmente da ***fonti eterogenee****, quindi non soltanto i dati strutturati, come i database, ma anche non strutturati, come* ***immagini****,* ***email****,* ***dati GPS****, informazioni prese dai* ***social network****.*

Le 4 (5) V dei Big Data

40 Zettabytes
(43 trilioni di GB) nel 2020
- Fonte IBM -

Volume
Quantità di dati

Dati sulla salute
Dati dei Social Network
Video - Facebook -
Twitter

Variety
Differenti tipologie di dati

Value
Valore

Velocity
Rapida elaborazione

Veracity
Qualità dei dati

Nel 2016
18,9 bilioni di reti connesse
- Fonte IBM -

Il valore degli investimenti
devono essere basati
su dati accurati e
portare miglioramenti
misurabili per ridurre i
costi

Percentuale molto
bassa di
corrispondenza per
interoperabilità e
affidabilità

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Verso una florida economia basata sui dati - 2/7/2014

Con il termine "big data" si fa riferimento a grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti. La gestione di questi dataset ad elevata variabilità e in tempo reale impone il ricorso a nuovi strumenti e metodi, quali ad esempio potenti processori, software e algoritmi.
In generale, l'analisi dei dati migliora i risultati, i processi e le decisioni. Contribuisce inoltre a generare nuove idee o soluzioni o a prevedere gli eventi futuri con maggiore precisione. Con il progresso tecnologico assistiamo alla riorganizzazione di interi settori di attività, che si basano sistematicamente sull'analisi dei dati.
Con il termine "innovazione guidata dai dati" si fa riferimento alla capacità delle imprese e degli organismi pubblici di utilizzare le informazioni derivanti da analisi dei dati migliorate per sviluppare beni e servizi migliori, in grado di semplificare la vita quotidiana di individui e organizzazioni, incluse le PMI

1. **Protezione dei dati personali e tutela dei consumatori** Il diritto fondamentale alla protezione dei dati personali si applica ai big data quando questi sono a carattere personale: il trattamento dei dati deve avvenire in conformità a tutte le norme applicabili in materia di protezione dei dati.
2. **Data mining** La Commissione sta esplorando le possibilità per migliorare l'innovazione guidata dai dati e basata sul data mining (o estrazione di dati), incluso il text mining, anche in relazione ai pertinenti aspetti legati al diritto d'autore.
3. **Sicurezza** La Commissione valuterà i rischi relativi alla sicurezza connessi ai big data e proporrà misure di gestione e attenuazione dei rischi, compresi orientamenti, ad esempio sulle buone pratiche per l'archiviazione sicura dei dati, al fine di promuovere una cultura della sicurezza in molti settori della società e contribuire a individuare e contrastare meglio gli attacchi informatici.
4. **Proprietà/trasferimento dei dati** In diversi settori, i requisiti in materia di ubicazione dei dati limitano il flusso transfrontaliero di informazioni e ostacolano la realizzazione di un mercato unico per il cloud computing e i big data.

Perché ci interessiamo ai Big Data e a quanto accade sulla rete Internet ?

La risposta è nella quantità di dati/informazioni esposti pubblicamente sulla rete.

Infatti, tutti i dati/informazioni esposti pubblicamente sulla rete potenzialmente costituiscono indicatori per query e aggregazioni.

IL GDPR

SL FABIANO

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

(C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita	Article 25 Data protection by design and by default
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, **volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.	1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as **data minimisation**, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.	2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.	3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Data Protection by Design co. 1

Data Protection by default co. 2

SANZIONI

la violazione dell'art. 25 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000,00 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

QUALIFICAZIONE DEI PRINCIPI

- Espressione del principio di accountability e quindi responsabilizzazione del titolare del trattamento
- Il titolare del trattamento è responsabile, fra l'altro, anche per la corretta applicazione dei principi contenuti nell'art. 25:
  a) data protection by design
  b) data protection by default
- Il paragrafo 3 conferma questo assunto, proprio perché il meccanismo di certificazione costituisce elemento per dimostrare la conformità e, quindi, limita la responsabilità del titolare.

OBBLIGO DI PROTEZIONE DEI DATI

Considerando n. 28

L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.

PSEUDONIMIZZAZIONE - MINIMIZZAZIONE

Art. 4 - Definizioni

«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Art. 5 - Principi applicabili al trattamento di dati personali

I dati personali sono:

…

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

ERRORE CONCETTUALE

minimizzazione = anonimizzazione ?

oppure

minimizzazione ≠ anonimizzazione

ANONIMIZZAZIONE

Esempio: un consiglio comunale offre una tessera con microprocessore agli utenti abituali del sistema di trasporto pubblico cittadino dietro pagamento di un certo importo. Il nome dell'utente compare per iscritto sulla superficie della tessera e, in forma elettronica, nel microprocessore. A ogni corsa la tessera dev'essere avvicinata all'apposito lettore installato, per esempio, sugli autobus e sui tram. I dati letti dal dispositivo sono controllati elettronicamente a fronte di quelli di una banca dati contenente i nomi delle persone che hanno acquistato la tessera di trasporto.

Questo sistema non rispetta appieno il principio di pertinenza poiché il controllo della legittimità dell'uso dei mezzi di trasporto da parte di un individuo potrebbe essere effettuato senza confrontare i dati personali presenti sul microprocessore della tessera con quelli di una banca dati. Sarebbe sufficiente, per esempio, disporre di un'immagine elettronica particolare, come un codice a barre, nel microprocessore della tessera che, dopo essere stata avvicinata al lettore, confermerebbe o meno la validità della tessera. Un simile sistema non effettuerebbe alcuna registrazione di chi ha utilizzato un determinato mezzo di trasporto e a che ora. Si creerebbe una situazione in cui non sarebbe raccolto alcun dato personale, soluzione ottimale ai sensi del principio di pertinenza, che comporta l'obbligo di minimizzare la raccolta dei dati.

MANUALE SUL DIRITTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

- I dati sono **anonimizzati** quando non contengono più alcun mezzo identificativo, mentre sono **pseudonimizzati** se i mezzi identificativi sono criptati.
- **A differenza dei dati anonimizzati, i dati pseudonimizzati sono dati personali**.

MANUALE SUL DIRITTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

2.1.3. Dati anonimizzati e pseudonimizzati

Secondo il **principio della conservazione** di dati per un periodo di tempo limitato, contemplato dalla direttiva sulla protezione dei dati nonché dalla Convenzione n. 108 (e discusso in maniera più approfondita nel capitolo 3), i dati devono essere conservati "*in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati*". Di conseguenza, i dati dovrebbero essere anonimizzati qualora un titolare del trattamento volesse conservarli dopo che fossero divenuti obsoleti e non più utili al soddisfacimento dello scopo iniziale.

MANUALE SUL DIRITTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

Dati anonimizzati

I dati sono anonimizzati **se tutti gli elementi identificativi sono stati eliminati da un insieme di dati personali**. Le informazioni non devono mantenere alcun elemento identificativo che, con un ragionevole sforzo, potrebbe servire a identificare nuovamente la persona o le persone interessate. Una volta resi completamente anonimi, **i dati non sono più ritenuti personali**. Se i dati personali non sono più utili al soddisfacimento dello scopo iniziale, ma devono essere conservati in forma personalizzata per motivi storici, statistici o scientifici, è possibile conservarli ai sensi della direttiva sulla protezione dei dati e della Convenzione n. 108, **a condizione che siano applicate adeguate misure di garanzia contro eventuali abusi**.

Regolamento UE 2016/679

Articolo 32 - Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, **si tiene conto in special modo dei rischi** presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Tecniche di anonimizzazione

Tecniche di anonimizzazione

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

0829/14/IT
WP216

Parere 05/2014 sulle tecniche di anonimizzazione

adottato il 10 aprile 2014

WP126

Il presente parere illustra le principali tecniche di anonimizzazione, ossia la **randomizzazione** e la **generalizzazione**. In particolare, il parere esamina l'aggiunta del **rumore statistico**, le **permutazioni**, la **privacy differenziale**, l'**aggregazione**, il **k-anonimato**, la **l-diversità** e la **t-vicinanza**. Ne illustra i principi, i punti di forza e di debolezza, nonché gli errori e gli insuccessi comuni connessi all'impiego di ciascuna tecnica.

Il parere esamina l'affidabilità di ogni tecnica sulla base di tre criteri:
i) è ancora possibile individuare una persona,
ii) è ancora possibile collegare i dati relativi a una persona, e
iii) è possibile dedurre informazioni riguardanti una persona?

Conoscere i principali punti di forza e debolezza di ciascuna tecnica è utile per decidere come progettare un processo di anonimizzazione adeguato in un determinato contesto. Viene presa in esame anche la **pseudonimizzazione** al fine di chiarire alcune insidie e convinzioni erronee: **la pseudonimizzazione non è un metodo di anonimizzazione**. Si limita a ridurre la correlabilità di un insieme di dati all'identità originaria di una persona interessata, e rappresenta pertanto una misura di sicurezza utile.

WP126

Il parere giunge alla conclusione che le tecniche di anonimizzazione possono fornire garanzie di protezione della sfera privata e possono essere utilizzate per creare efficaci procedure di anonimizzazione, **ma soltanto se la loro applicazione viene progettata in maniera adeguata** – nel senso che i requisiti preliminari (contesto) e l'obiettivo o gli obiettivi della procedura di anonimizzazione devono essere definiti in modo chiaro per ottenere l'anonimizzazione desiderata e produrre al contempo dati utili. **La soluzione ottimale dovrebbe essere decisa caso per caso, se possibile utilizzando una combinazione di tecniche diverse e tenendo conto delle raccomandazioni pratiche formulate nel presente parere.**

Infine, i responsabili del trattamento **devono essere consapevoli** che un insieme di dati resi anonimi **può comunque presentare rischi residui per le persone interessate**. Di fatto, da un lato anonimizzazione e reidentificazione sono argomenti attivi di ricerca e vengono regolarmente pubblicate nuove scoperte in materia e, dall'altro lato, persino i dati resi anonimi, come le statistiche, possono essere utilizzati per arricchire i profili esistenti delle persone, determinando quindi nuovi problemi di protezione dei dati. **L'anonimizzazione non va pertanto considerata un'operazione una tantum e i relativi rischi dovrebbero essere oggetto di un riesame periodico da parte dei responsabili del trattamento.**

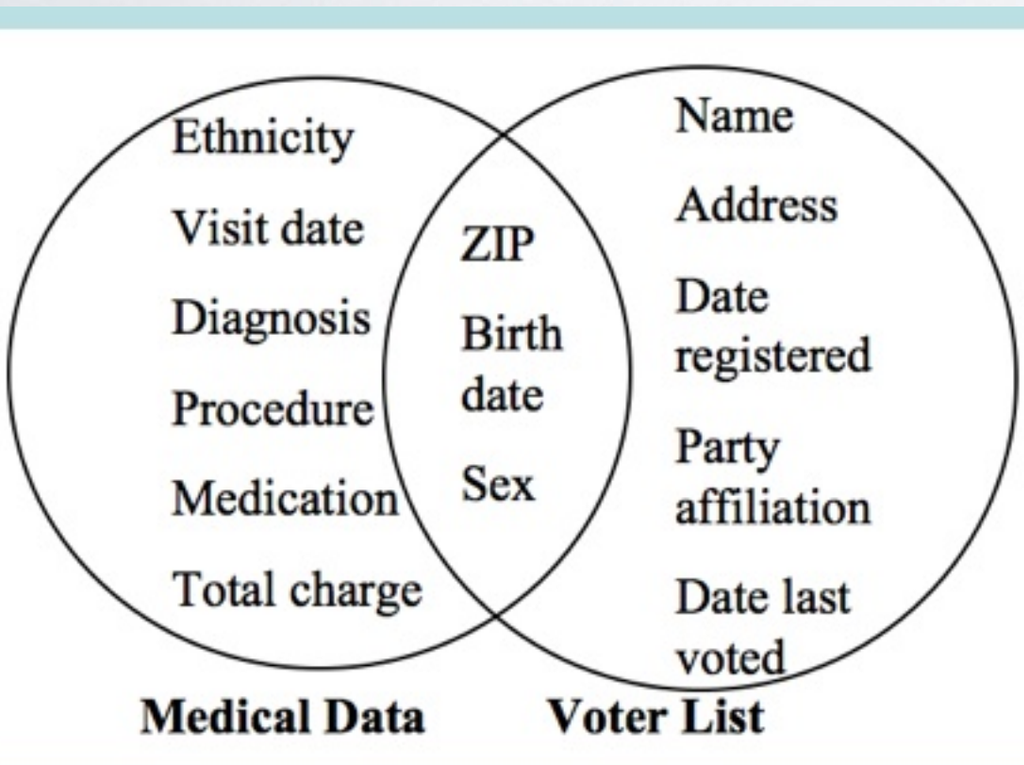
SONO SICURE LE TECNICHE DI ANONIMIZZAZIONE ?

Potrebbero non esserlo quando, attraverso l'uso di algoritmi basati su complesse operazioni matematiche, è possibile comunque rendere un soggetto identificabile.
Sono noti gli attacchi che hanno reso re-identificabili i dati.

LATANYA SWEENEY

Professoressa all'Università di Harvard

Nel 1997 con il contributo dal titolo "Computational Disclosure Control A Primer on Data Privacy Protection " Dimostra che:



Spesso le organizzazioni rilasciano e ricevono dati specifici della persona con tutti gli identificatori espliciti, come nome, indirizzo e numero di telefono, se rimossi sul presupposto che la privacy viene mantenuta perché i dati risultanti sembrano anonimi. Tuttavia, nella maggior parte di questi casi, i dati rimanenti possono essere utilizzati per reidentificare le persone ….

IL CASO NEW YORK TAXI

Il set di dati di tutte le corse in taxi del New York Taxi nel 2014 è stato de-identificato tramite l'identificazione inversa della pseudonimizzazione.
Uno stagista di dati scientifici a Neustar ha scoperto di poter trovare le foto delle celebrità che entrano o escono dai taxi con il numero di taxi.
Ha usato indirettamente l'identificazione di informazioni, il numero di taxi, l'ora e la data, per individuare le corse specifiche nel set di dati rilasciato dalla commissione di New York City Taxi e Limousine.
Da questi 3 identificatori indiretti, il tirocinante ha poi utilizzato il set di dati per identificare la posizione di prelievo, la posizione di destinazione, l'importo pagato e persino l'importo di punta.

IL CASO NETFLIX

Nel 2006, Netflix ha rilasciato pubblicamente cento milioni di record che rivelano centinaia di migliaia di voti degli utenti dal 1999 al 2005 e ha offerto un premio di un milione di dollari al primo team per migliorare in modo significativo l'algoritmo di raccomandazione sui filmati di Netflix.
Sebbene i dati non contenessero identificativi diretti, nel corso delle settimane dal rilascio dei dati, due ricercatori sono stati in grado di re-identificare un sottogruppo di persone specifiche facendo riferimento incrociato ai dati di Netflix con le valutazioni di IMDB.com.
Usando solo sei valutazioni di film oscuri, i ricercatori hanno re-identificato le persone l'84% delle volte (se si trovassero in entrambi i set di dati).
Includendo un tempo approssimativo della valutazione è stato permesso l'identificazione il 99% delle volte.
Anche se questo ha funzionato solo per re-identificare gli utenti Netflix che avevano anche account IMDB, le informazioni di Netflix potevano essere confrontate con le preferenze dei social media trovate su app di incontri online e Facebook per risultati simili.

IL CASO AOL

Nel 2006 AOL ha rilasciato 20 milioni di query di ricerca per 650.000 utenti, da tre mesi di dati.
AOL ha tentato di ripulire i dati di qualsiasi identificatore diretto o indiretto: ha cancellato identificatori diretti come nomi utente e indirizzi IP.
Per preservare l'utilità dei dati, AOL ha sostituito tali informazioni con numeri di identificazione univoci tramite pseudonimizzazione.
Poiché ogni utente aveva un numero univoco, i risultati di ricerca di ciascun utente potevano essere visualizzati come un gruppo.
Poco dopo l'uscita, due giornalisti del New York Times sono riusciti a rintracciare una vedova di sessantadue anni in Georgia analizzando le sue ricerche AOL.

Differential Privacy

DIFFERENTIAL PRIVACY

Differential privacy is a definition of privacy tailored to the problem of privacy-preserving data analysis.

Data cannot be fully anonymized and remain useful.

Cynthia Dwork - Aaron Roth

The Algorithmic Foundations of Differential Privacy

WP126

La **privacy differenziale** appartiene alla famiglia delle tecniche di randomizzazione, ma adotta un approccio diverso: mentre l'inserimento del rumore statistico interviene prima, al momento dell'eventuale pubblicazione dell'insieme di dati, la privacy differenziale può essere utilizzata quando il responsabile del trattamento genera opinioni anonimizzate di un insieme di dati e conserva al contempo una copia dei dati originali. Le opinioni anonimizzate sono solitamente generate attraverso un sottogruppo di interrogazioni per terzi specifici. Il sottogruppo presenta una certa dose di rumore statistico casuale aggiunto appositamente a posteriori.

DIFFERENTIAL PRIVACY

Nominativo	Data di nascita	Indirizzo	Città	Fratture
Antonio Rossi	10/01/1960	Via Verdi, 1	**Roma**	**SI**
Ugo Neri	20/10/1970	Via Rossi, 5	Viterbo	NO
Michele Verdi	**15/05/1980**	Via dei Faggi, 12	**Roma**	NO
Luigi Moro	**25/08/1980**	Corso Genova, 10	Milano	**SI**

Supponiamo che si possano effettuare solo interrogazioni d'insieme (es. "Quante persone vivono a Roma?" - "Quante persone sono nate nel 1980?" - "Quante persone hanno subito fratture?"). Con la privacy differenziale si inserisce un **elemento di casualità** alle interrogazioni del database che induce a rendere indistinguibili le risposte. Alla base c'è una complessa formula matematica che spiega e giustifica.

DIFFERENTIAL PRIVACY

Una definizione matematica di Differential Privacy

$$p(Z = z|X = x_1) \leq e^{\varepsilon} p(Z = z|X = x_2)$$

Cynthia Dwork utilizza un approccio con introduzione di rumore secondo la distribuzione di Laplace

WP126

La privacy differenziale suggerisce al responsabile del trattamento la quantità e la forma di rumore statistico che va aggiunto per ottenere le garanzie di tutela della sfera privata richieste. In tale contesto, è particolarmente importante continuare a controllare (almeno per ogni nuova interrogazione) che non sussista la possibilità di identificare una persona nell'insieme dei risultati dell'interrogazione.

Occorre tuttavia chiarire che le tecniche di privacy differenziale **non modificano i dati originari** e pertanto, finché questi permangono, il responsabile del trattamento è in grado di identificare le persone all'interno dei risultati delle interrogazioni di privacy differenziale tenendo conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati. **Tali risultati vanno trattati alla stregua di dati personali.**

Differential Privacy


Quando l'intelligenza artificiale ha la forma di una...


La piattaforma di crowdfunding Ulule vola oltre i 100...

Oggi e domani aperta al pubblico la Facebook Election Lounge


Una rete
Luna: la
nel 2019.

DOPO WWDC

Il mistero svelato della privacy differenziale: ecco come funziona

–di **Luca Tremolada** | 27 giugno 2016

Differential Privacy

15/6/2016

L'intelligenza artificiale non sostituirà i lavoratori, ma li affiancherà

Con l'intelligenza artificiale, le auto autonome si possono trasformarsi in armi

Da Google un algoritmo per prevenire le malattie cardiache

In Francia un'etichetta per combattere l'obsolescenza programmata dei gadget

Vodafone testa il primo sistema IoT per il monitoraggio e la sicurezza dei droni

Cos'è la privacy differenziale di Apple e perché potrebbe cambiarci la vita

SL FABIANO

Differential Privacy

macOS Sierra: Condividere le informazioni di analisi con Apple

Le informazioni di analisi possono essere inviate ad Apple quando segnali un problema; puoi scegliere o meno se condividere tali informazioni.

Informazioni sull'analisi e sulla privacy

Puoi aiutare Apple a migliorare la qualità dei suoi prodotti e servizi, tra cui Siri e altre funzionalità intelligenti, consentendo di eseguire l'analisi dei dati di utilizzo del dispositivo e del tuo account iCloud.

Col tuo consenso, macOS può raccogliere automaticamente le informazioni di analisi dal Mac e inviarle a Apple per aiutare a migliorare la qualità e le prestazioni dei suoi prodotti. Le informazioni vengono inviate ad Apple solo dopo il tuo consenso e in formato anonimo.

Puoi anche consentire l'analisi di utilizzo e dei dati del tuo account iCloud per aiutare Apple a sviluppare a migliorare Siri e altre funzionalità intelligenti. L'analisi dei dati del tuo account iCloud, inclusi frammenti di testo di messaggi e-mail o altri dati simili nel tuo account, viene eseguita solamente dopo che i dati sono sottoposti a tecniche che tutelano la privacy, come la privacy differenziale, in modo che non siano associati a te né al tuo account.

La pseudonimizzazione

MANUALE SUL DIRITTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI

Dati pseudonimizzati

Le informazioni personali contengono elementi identificativi come nome, data di nascita, sesso e indirizzo. Quando le informazioni personali vengono pseudonimizzate, gli elementi identificativi sono sostituiti da uno pseudonimo, che si ottiene, per esempio, crittografando gli elementi identificativi contenuti nei dati personali. I dati pseudonimizzati non sono esplicitamente menzionati nelle definizioni giuridiche della Convenzione n. 108 o nella direttiva sulla protezione dei dati. …

Si tratta di un effetto che può essere ottenuto mascherando i dati mediante uno pseudonimo. Per chiunque non sia in possesso della chiave di decifratura, i dati pseudonimizzati sono identificabili con difficoltà; il collegamento a un'identità esiste ancora sotto forma di pseudonimo associato alla chiave di decifratura. …

PSEUDONIMIZZAZIONE

Si utilizza la crittografia per evitare che il dato sia riconducibile alla persona e, quindi, identificabile.

Alcune soluzioni crittografiche:

- algoritmo RSA (pubblicato nel 1978 - brevetto del 1983 scaduto nel 2000)
- algoritmo ElGamal (pubblicato nel 1984 - impiegato nello standard della firma digitale e nello standard S/MIME per gli allegati della posta elettronica)
- Infrastruttura PKI (Public Key Infrastructure)

PKI

I soggetti:

- Certification Authority (Autorità di certificazione)
- End Entity (utenti finali)
- Registration Authority (Autorità di registrazione)
- Gestori delle liste di revoca

FUNZIONE DI HASH

Algoritmo matematico che mappa dei dati di lunghezza arbitraria (messaggio) in una stringa binaria di dimensione fissa chiamata valore di hash, ma spesso viene indicata anche con il termine inglese message digest (o semplicemente digest). Tale funzione di hash è progettata per essere unidirezionale (one-way), ovvero una funzione difficile da invertire: l'unico modo per ricreare i dati di input dall'output di una funzione di hash ideale è quello di tentare una ricerca di forza-bruta di possibili input per vedere se vi è corrispondenza (match).

Fonte: Wikipedia

PSEUDONIMIZZAZIONE

Nominativo	Data di nascita	Indirizzo	Città	Fratture
AY#006V@	10/01/1960	Via Verdi, 1	**Roma**	**SI**
@75%VKL		Via Rossi, 5	Viterbo	NO
§6432#@			**Roma**	NO
921@#%$				**SI**

Alcuni dati o set di dati sono stati criptati con un sistema a doppia chiave asimettrica

FUNZIONE DI HASH

In applicazione del principio "by design", i criteri da considerare nel sistema della pseudonimizzazione dovranno offrire la tutela dell'interessato:

1. irreversibilità del processo di codifica + security policies
2. impact risk assessment, gestione del rischio di impatto in maniera da evitare falsi positivi (segnalare come falso ciò che in realtà è vero - es. antivirus che segnala un software malevolo che non lo è) + impatto sull'interessato

Internet of Things

Internet of Things? Sconosciuta a 6 universitari su 10

Pubblicato il 15 marzo 2018 in Innovazione, Vicenza

Sei studenti universitari su 10, e qualcuno in più, non hanno mai sentito parlare di **Internet of Things**. Altrettanti non hanno dimestichezza con i Big Data e in ambito Blockchain le cose vanno ancora peggio. Sono i dati emersi durante il seminario "Digital As_L: Competenze a prova di futuro", promosso da **Niuko Innovation & Knowledge** a Villa Valmarana Morosini di Altavilla Vicentina la mattina del 15 marzo. È stata l'occasione per un centinaio di studenti dell'IIS De Nicola di Piove di Sacco (Padova), ISS Ceccato di Montecchio Vicentino e ITS Kennedy, ma anche per docenti e imprenditori, di sentire parlare **Fabio Bocchi** di University2Business. Autore di una ricerca che rivela il "buco" dei giovani italiani per quanto riguarda l'innovazione.

Internet of Things

Scott Bedford/Shutterstock

Definire l'IoT è una sfida in ragione della sua complessità tecnica e concettuale.
Una delle definizioni scientifiche l'ha fornita l'ITU:
"***a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies***"
(Recommendation ITU-T Y.2060 - 06/2012).

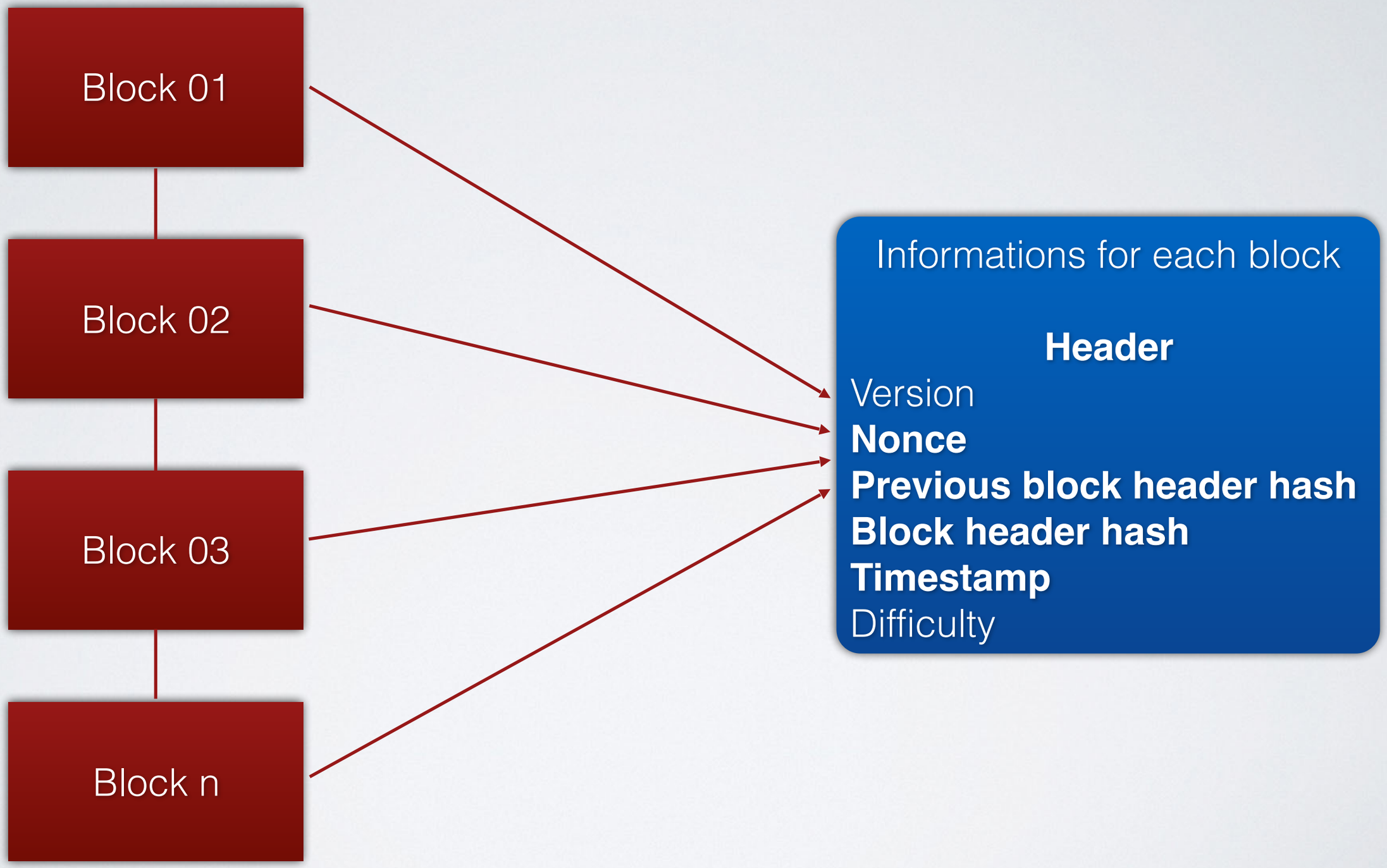
L’ecosistema IoT

L’IoT sta evolvendo come un ecosistema all’interno del quale si sviluppano tecnologie per l’erogazione di servizi.

La blockchain è un “*distributed database*” (*ledger)* e costituisce un pilastro di tale ecosistema. Essa si evolve a tal punto da poter parlare di “**blockchain as a service**”.

Electronic Identification (eID) nella blockchain.

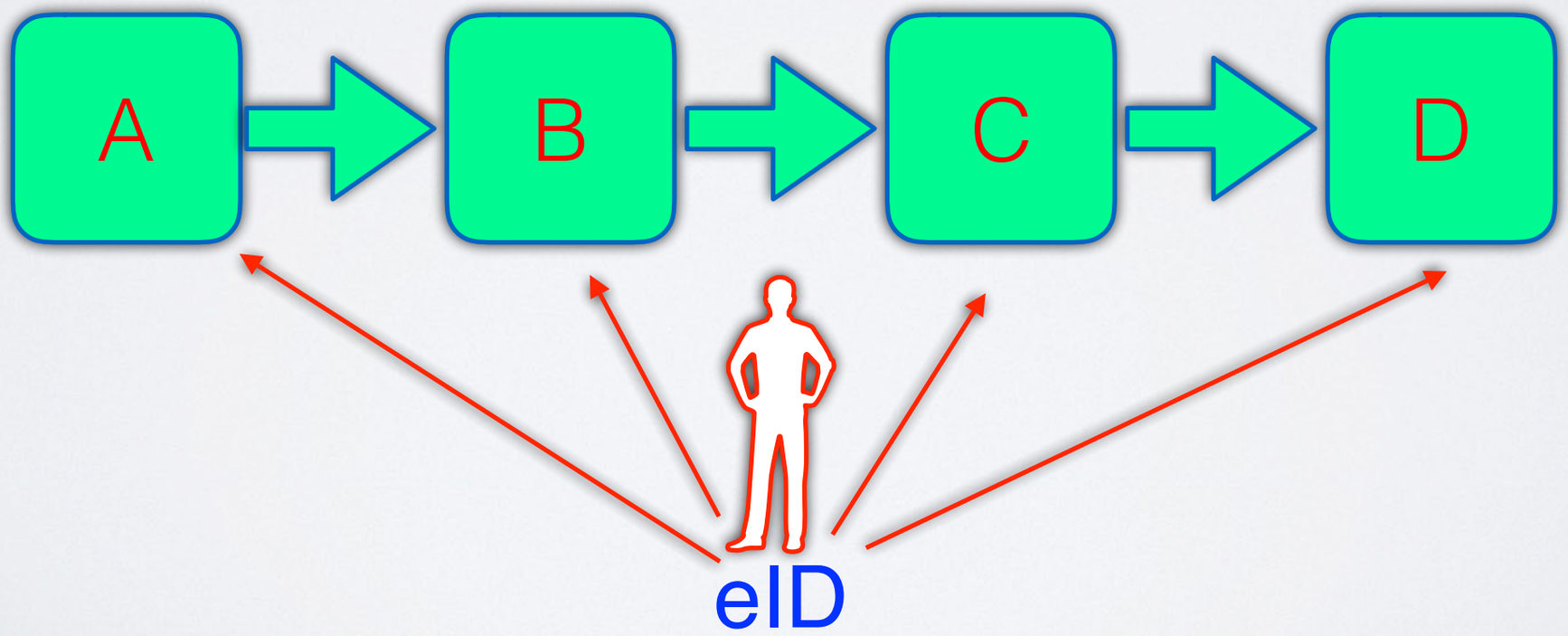
La struttura della blockchain



La prospettiva delle applicazioni della blockchain

Electronic Identification (eID) nella blockchain

Blockchain as a Service



Security & Privacy / Data Protection

Security ≠ Privacy

Quale privacy nella blockchain ?

Alcuni quesiti:

- Chi è il titolare del trattamento ?
- L’interessato è proprietario del nodo e anche titolare del trattamento dei dati personali ?
- Quali profili di responsabilità per la violazione dei dati personali (art. 34 Regolamento EU 679/2016) ?

Machine Learning e Artificial Intelligence

L'utilizzo del *Machine Learning* può favorire lo sviluppo di un sistema di gestione della protezione dei dati personali (DPMS) che, sfruttando l'intelligenza artificiale (*AI*), consentirà di raggiungere risultati nel pieno rispetto degli approcci metodologici (by design e by default) con l'implementazione di misure di sicurezza adeguate riducendo i rischi.

Fenomeni “smart”

- Smart Grid
- Smart City
- Smart Car
- Smart Home
- ….

Fenomeni “smart”

- Smart Grid
- Smart City
- Smart Car
- Smart Home
- ….

Esempio di blockchain

Blockchain

Block: # 1

Nonce: 11316

Data:

Prev: 0000000000000000000000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d0600e2cbb

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2cbb

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5

Mine

Le tipologie di blockchain

1. **Public blockchain** (tutti possono accedere e fare transazioni);
2. **Private blockchain** (il controllo è da parte dell'organizzazione);
3. **Consortium/Combined blockchain** (il controllo è da parte di alcuni nodi);

PoW - PoS

Proof of Work (PoW): si richiede che gli utenti della blockchain effettuino qualche attività di lavoro (work) in termini di potenza computazionale per il processo di mining (validazione delle transazioni - coincidenza delle impronte di hash).

Proof of Stake (PoS): è un modo differente per validare le transazioni basato sul consenso (il creatore di un blocco è scelto sulla base del suo "patrimonio" che viene messo a disposizione per validare i blocchi).

I Principi

Articolo 5
Principi applicabili al trattamento di dati personali

a) «liceità, correttezza e trasparenza»
b) «limitazione della finalità»
c) «minimizzazione dei dati»
d) «esattezza»
e) «limitazione della conservazione»
f) «integrità e riservatezza»

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Tracciamento e profilazione

COOKIES

Cookie di tracciamento

- HTTP cookies
- Javascript cookies
- HTML5 Local Storage 1st party cookies
- HTML5 Local Storage 3rd party cookies
- IndexedDB
- Silverlight Isolated Storage
- Flash Local Shared Object
- Web beacons
- Ultrasound beacons
- Pixel tags

TECNICHE DI TARGETING

- Behavioural targeting / advertising
- Contextual targeting
- Demographic targeting
- Geographic targeting
- Time-based targeting (visualizzazione annunci in un momento particolare della giornata)
- Emotional targeting (riconoscimento del corpo)
- Retargeting (tecniche per riconoscere gli utenti al di fuori del dominio)

USER AGENT

☑ Mail user agent (MUA)
☑ Browser fingerprint

Verifica:

- https://panopticlick.eff.org
- https://extensions.inrialpes.fr/

I DISPOSITIVI MOBILE

- **Dispositivi mobile**
  - **smartphone e tablet**
    - **Device ID**
      - **Android ID**
      - **Universal Device ID (UDID)**
      - **Advertising ID**
        - **Google advertising ID (GaID)**
        - **Identifier for Advertising (IDFA)**
  - **app c.d. amiche (trasmettono dati per finalità di marketing)**
  - **geolocalizzazione**
  - **dati EDIF nelle foto**
  - **impostazioni della privacy**

LETTURE CONSIGLIATE

- Privacy by Design: l'approccio corretto alla protezione dei dati personali - http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2015-04-20/privacy-by-design-approccio-corretto-protezione-dati-personali-123915.php

Grazie per l’attenzione

Avv. Nicola Fabiano

info@fabiano.law

www.fabiano.law

@nicfab

/nicfab

/nicfab